Study on Mobile Large Data Storage Security in Cloud Computing Environment

Xianwei Li

Information Engineering Department, ShanDong Polytechnic, Jinan 250001, China

xianwei@sina.com.cn

Keywords: Cloud computing, data security, mobile large data, information flow control, trusted cloud computing.

Abstract. In this thesis, data security in cloud computing is regarded as the research object. First of all, the definitions, model, structure, application, research organization and related knowledge of cloud computing is introduced. Then, the data security assurance methods which used in this thesis including symmetric and asymmetric encryption system, attribute-based encryption algorithm and Merkle Hash Tree are discussed. The security challenge, advantage, protective measures and security architecture of data security based in cloud computing environment are summarized with many cloud computing characteristics, such as massive, virtualization, dynamics and expansibility.

Introduction

Cloud computing provides a large number of IT resources such as hardware and software as a service to users through the network. In cloud computing service model, users host data and application to the cloud, due to the cloud service transparency, they lose control of the data. Because it is difficult to assess cloud provider's credibility for users, data security has become the primary concern in cloud computing.

Since cloud computing does related operations based on user's service request, authentication between users and cloud providers can avoid illegal access from assumed identity. Whereas, due to the large number of users, how to realize safe and efficient authentication is the concern for and users and service providers. [1] Having been authenticated, users can use the data storage commission computing services. Users upload large amounts of data to the cloud and cloud service providers to calculate without the local copy stored. Although the cloud service provider is with strong technical strength and maintenance, it is not possible to completely prevent data damage or leakage occurs. For static storage of data, due to the mass of data, it is no longer applicable to verify integrity after downloading data to local in traditional way. If users find data integrity is compromised, they can only pray the cloud service provider's disaster recovery mechanism works. Because of the characteristics of multi-tenant in the cloud, user’s access data and compute through the service process for dynamic data in computing service, the process carrier of shared access become focal point of authority. [2] But it is difficult to achieve effective isolation and control of different users' data by shared permissions on OS level, data isolation mechanism of application solely is easily bypassed, so data confidentiality and integrity in multi-tenant environment remain to be resolved. If the data disclosure really happens, it is a key issue to charge service providers' responsibility. [3] Current accountability mechanisms need details of cloud services, which are related to cloud service providers' trade secrets, consequently it is difficult to achieve. In addition, due to the lack of trusted protection mechanism, security mechanism may be attacked, tampered or bypassed, accordingly it fails.

The essence of the cloud data security problem is the trust management between data owner and service provider, certain data constraints should be formed between them. They achieve certain data use agreement through reputation and technical means of restraint, contribute to the legitimate use of data and prevent from destroying. Users can choose to rely on service provider side by reaching a mutually satisfactory security mechanism to maximize safety and security, service providers will not

have a place to live in once he lost credibility. In this context, cloud service providers are willing to cooperate with users to take data security protection technology, and never do intentional destruction of user data, but they may hide data safety accident. From this point of view, the thesis studies on the authentication, static memory data protection, dynamic calculation data protection and trusted cloud computing, etc. are studied, to provide comprehensive data security protection for cloud users.

Technology of storage security

In the face of data storage security issues of the cloud computing, we study data integrity and data privacy protection in this paper.

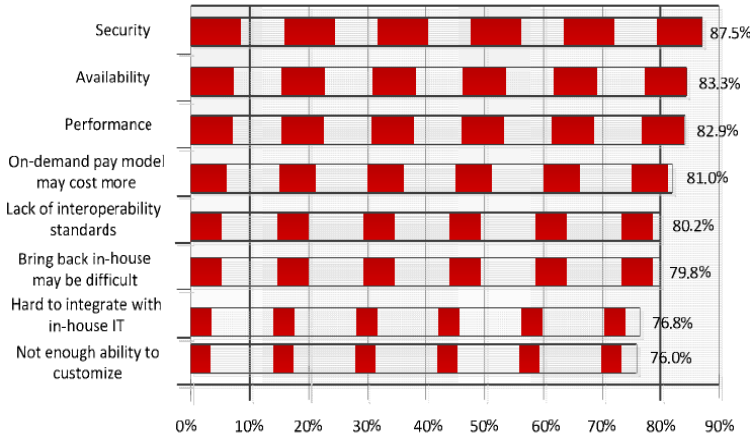

Fig. 1 The key problem of user attention

According to the key problem of user attention (Fig. 1), we can obtain that users are mostly focus on data security.

In the side of data integrity protection, we proposed the algorithm of proofs of irretrievability: M-POR which based on the message authentication code(MAC) with the purpose of making the user learn the data state in the cloud, algorithm generates sentinels through MAC and verify the data integrity through the process of "challenge-respond-verify". [4] Sentinels not only can verify the data integrity but also can position the error message. We also bring in RS code so that we can recovery data when the proportion of damaged data is not large and take into account of redundant replica of cloud computing.

In the side of data privacy protection, aiming at the privacy of text data, we proposed the MC-R strategy. MC consists of three modules: data masking, data concealing and data marker. [5] MC prevents data leakage when data is uploading or downing through masking and concealing data in the client, R enciphers data with the computing advantage of cloud computing in the cloud using the public key uploading from the client.

Table 1 Emergency computing resource availability tables

Resource site	Resource name	CPUs
UC/ANL	IA32/IA64	316/316
NSCA	Mecury	1744/1744
TACC	Frost	256/2048
NCAR	Lonestar	64/5840
IU	BigRed	TBD/3072
Total	5	2380/13020

Key technology

Research on the key technology of secure cloud data storage auditing scheme, i.e data aggregate signature algorithm. After analysis of existing works, we come with a new identity-based aggregate signature scheme, where each user keeps less number of private keys and the computational

complexity. Further more, we propose a new efficient identity-based aggregate signature scheme with both advantages ofbatch-verfication signature and aggregate signature. It could offer large scale of data verification in the multi-user setting with high efficiency. In particular, this scheme is quite suitable for data verification in multi-user and multi-cloud settings of cloud computing.

On this basis, according to the data storage's dynamic operation characteristics and less of verification support in cloud computing environment, the thesis has put forward a scheme which is based on the Merkle Hash Tree structure. The main ideas and safe assumption of the scheme are introduced. Also the pretreatment and validation method of the file and data dynamic operation process including insertion, modification and deletion are described. The scheme is data file's proposed access control problem analyzed as well. In addition, due to solving the cloud computing environment, the thesis has a solution which is based on attribute-based encryption algorithm and introduced the main ideas and safe assumption of the scheme. The participants and related definitions are described. The thesis has designed initialization of scheme, file access and the change of access permission in details. Finally, the scheme is also analyzed.

Data storage strategy

Here, we put forward three kinds of mobile storage model.

Mobile data management architecture based on mobile database (MDMA, Mobile Data Management Architecture) and storage management solution (SMS, Storage Management Solution) (Fig. 2)are proposed. Mobile database is the most efficient mode for mobile distributed environment data organization and storage, which will provide data foundation of mobile business operations, because mobile applications are implemented based on mobile databases. Aiming at the characteristics of mobile environment, mobile data management architecture and storage management solution are proposed, and the pre-fetch and replication, cache synchronization, transaction process, concurrence control, broadcast mechanism and other key technologies are discussed. These will provide available and conventional runtime methods for the data storage and management under mobile environment.

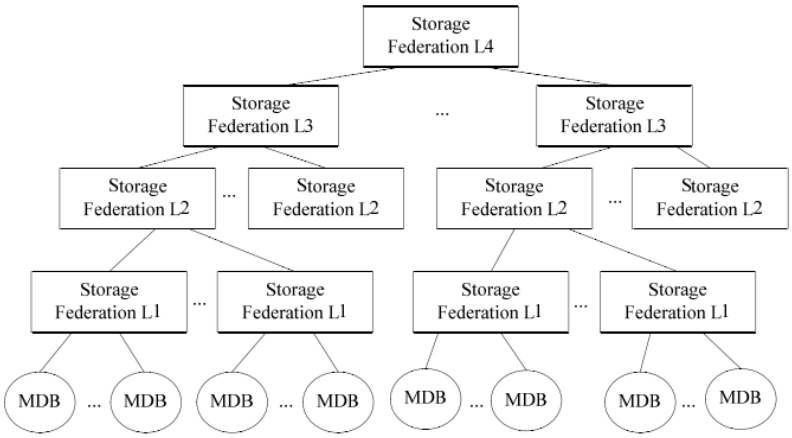

Fig. 2 SMS

A model of hierarchical storage system based on wireless mesh network (HSSWMN, Hierarchical Storage System over Wireless Mesh Network) (Fig. 3) is proposed.

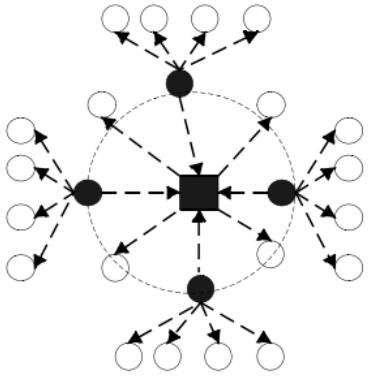

Fig. 3 Wireless Mesh network architecture unit

Firstly, the dissertation proposes the hierarchical storage system model based on wireless mesh network (HSSWMN), and the storage model, access algorithms and performance optimization methods are analyzed and researched. Secondly, name space and metadata service, search and looking for service, registration and logout, scalability, load balance, fault tolerant, data safety, replication and cache mechanism, topology reconstruction of HSSWMN are researched. At last, by the simulation analysis, simulation testing discloses that the delay, throughput, error code and etc, performance analysis is carried for the feasibility, availability and reliability of HSSWMN storage system.

A QoS cross layer model of storage service of mobile environment oriented (QCLMSS, QoS Cross Layer Model of Storage Services) (Fig. 4), and QoS guarantee algorithm of storage service (QASS, QoS Guarantee Algorithms of Storage Service) are proposed. The dissertation first does research on the QoS technologies of mobile environment storage service, analyzes the properties and relations between layers. Secondly, the QoS guarantee algorithms and performance model are proposed, and researches are done on QoS guarantee algorithms. At last, Global optimization, local optimization, mluti-state optimization, and self-adaptive optimization algorithms are proposed, and analysis and comparation of the mobile storage system QoS examples are analyzed, simulation test and analysis research is taken on disk I/O performance of wired network and wireless network access mode.

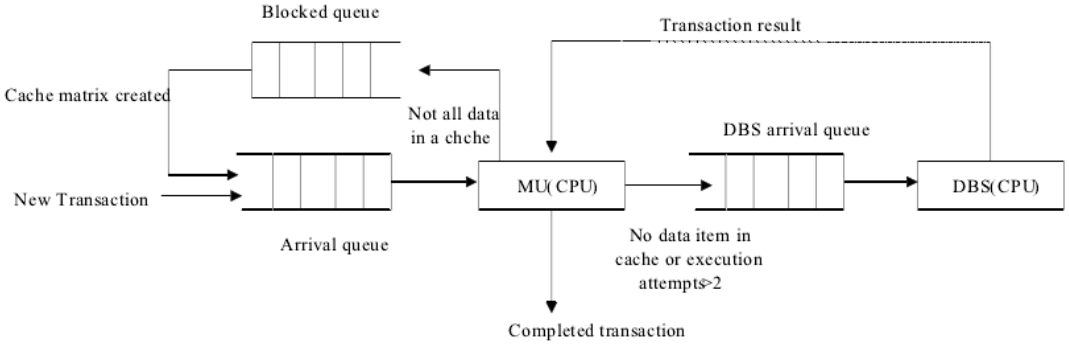

Fig. 4 HSSWMN

Conclusions

Firstly, this paper focuses on the current research of cloud storage security. The technical aspects of the security concern are confidentiality, integrity, availability, monitoring and audit. In this paper, current research on cloud storage security is summarized and introduced according to the security properties above. Then, this paper introduces a file-share method to solve the data storage problem. The method focuses on the confidentiality, integrity and key distribution and sharing problem.

References

[1] Frank Gens, Rebert Mahowald, Richard L.Villars et al. Cloud computing 2010 An IDC Update. IDC Executive Telebriefingp, 2009, 09.

[2] Shulman-Peleg A. Harnik D, Pinkas B. Side Channels in Cloud Services Deduplication in Cloud Storage. IEEE Security and Privacy Magazine, pedal issue of Cloud Security, 2010, 8(6): 40-47.

[3] Delettre C, Boudaoud K. and Riveill M. Cloud Computing, Security and Data Concealment. International Conference on Information Science and Cloud Computing, 2011: 424-431.

[4] Yang J S and Choi H K. IP Based Security Architecture of Virtual Network in Cloud Computing System. Wireless Communications and Mobile Computing Conference, 2012: 709-715.

[5] Almorsy M, Grun J and Ibrahim A S. Collaboration-Based Cloud Computing Security Management Framework. 2011 IEEE 4th International Conference on Cloud Computing, 2011: 364-371.